

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A SEARCH
AND SEIZURE WARRANT**

I, Ray D. Haney III, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 900 PROVIDENCE STREET, STAFFORD, VIRGINIA 22554 (hereinafter, "SUBJECT RESIDENCE") as further described in Attachment A, incorporated by reference herein, and for the items described in Attachment B, incorporated by reference herein.

2. Your Affiant, Task Force Officer (TFO) Ray D. Haney III is a Deputy Sheriff with the Stafford County Sheriff's Office in Stafford County, Virginia, and was duly sworn as a law enforcement officer at all times referred to herein. Your Affiant is currently assigned to the Stafford County Sheriff's Office Special Investigation Unit (SIU), which includes Vice/Narcotics, and is a sworn Task Force Officer for the United States Drug Enforcement Administration (DEA). Your Affiant has been a police officer for 28 years. During those 28 years your Affiant has investigated numerous narcotic cases, specifically including, but not limited to, cases involving users, dealers and traffickers of illegal narcotics, on both the state and federal level. Your Affiant has investigated cases involving money laundering and organized crime, in which your Affiant made arrests and obtained convictions for such. Your Affiant has received both basic and advanced training from local, state, and federal law enforcement agencies. Your Affiant has received basic narcotics identification training at the Rappahannock Regional Criminal Justice Academy.

3. I am a Task Force Officer with the Drug Enforcement Administration (DEA) and have been since January 8, 2019. I am currently assigned to the DEA High Intensity Drug Trafficking Area (HIDTA) Task Force located in Reston, Virginia. As such, I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United State Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, the offenses enumerated in Title 18, United States Code, Section 2516.

4. During my time in law enforcement, I have applied for and received numerous search warrants and have participated in the execution of numerous arrest and search warrants in the investigation of narcotics and organized crime related offenses, resulting in the prosecution and conviction of numerous individuals and the seizure of illegal drugs, weapons, stolen property, and other evidence of criminal activity. Additionally, I have received specialized training in the area of drug identification and illegal drug trafficking enforcement. I have attended classes and courses conducted by the DEA regarding the importation, transportation, and distribution of illegal drugs. I am knowledgeable about state and federal drug laws.

5. The facts and information contained in this affidavit are based upon my personal knowledge and observations during the course of this investigation, as well as the observations of other federal agents and individuals involved in this investigation. All observations not personally made by me were relayed to me by the individuals who made them or were conveyed to me by my review of the records, documents, and other physical evidence obtained during the course of the investigation. The inferences and conclusions I draw from the evidence included in this affidavit are what I believe based on my training, experience, and knowledge of the investigation.

PROBABLE CAUSE

6. This affidavit is submitted in support of an application for a search warrant authorizing the search of the SUBJECT RESIDENCE fully identified in Attachment A, incorporated by reference herein, for the items specifically described in Attachment B, which is incorporated by reference herein, and which constitute evidence, fruits and instrumentalities of illegal drug trafficking and a conspiracy to do the same in violation of Title 21, United States Code, Sections 841(a)(1) and 846.

7. The information contained in this affidavit is not intended to include each and every fact and matter observed by or known to the United States and its agents. The facts and information contained in this affidavit are based upon my personal knowledge, information obtained from local, state, and federal law enforcement officers (collectively “agents”), and information provided by reliable sources of information. The observations in this affidavit that were not my own were relayed to me directly by the person who made them. Information provided by sources of information has been corroborated by independent information where possible and the information provided by these sources upon which I relied has been determined to be reliable.

8. On October 2, 2023, your affiant began investigating a United Parcel Service Package (UPS) that was delivered to a specific address in Stafford County, bearing UPS tracking number of 1Z2173W30104014016 (“Package 1”). The recipient of this package was not expecting a package, however because Package 1 was addressed to them, in their name, they opened Package 1 and found that it contained a large vacuum sealed bag of what appeared to be fentanyl pills. The recipient contacted the Sheriff’s Office and Deputy Leckemby collected Package 1 that contained suspected fentanyl pills. Deputy Leckemby turned over Package 1 to your Affiant for further investigation. Package 1 contained approximately 15,000 fake blue

oxycodone pills, suspected to be fentanyl pills, weighing approximately 1,680 grams. These pills have an estimated street value of approximately \$300,000.00

9. Your affiant determined that Package 1 was originally shipped from a Kimberly Garcia of 4509 Pepperwood Avenue, Long Beach, California 90808 and was addressed to a Kim Stevens at "19 Wayside Court, Stafford, Virginia 22554." Package 1 was shipped on September 28, 2023, and was expected to ship next day air. The sender paid \$150.00 cash to ship Package 1. Package 1 was shipped from the UPS Store # 7586 Hawaiian Garden, California. On September 29, 2023, UPS attempted to deliver Package 1 to 19 Wayside Court Stafford, Virginia, however this address was a vacant address and UPS did not leave the package. UPS located another address in Stafford for the named addressee and delivered Package 1 to the address for the named addressee. That individual subsequently turned Package 1 over to the Sheriff's Office.

10. On October 3, 2023, your Affiant obtained information regarding Package 1 from UPS Store # 7586. According to UPS Store records, a female had called from phone number 540-282-0088 to UPS Store # 7586 asking about Package 1 and why it had not been delivered. The number that the female called for the UPS store was not the listed business number for the UPS store, and would have only been found on the receipt, which was printed at the time the package was delivered to the UPS store to be shipped or on prior packages that may have been delivered.

11. On October 3, 2023, your Affiant received information from UPS Store #6490 which is located in Lakewood, California, that on July 12, 2023, a Kimberly Garcia mailed a parcel to 105 Fiddlers Court, Stafford, Virginia 22554. Also, on July 27, 2023, a Jocelyn Lopez sent a parcel from UPS Store #6490 to the same address of 105 Fiddlers Court, Stafford, Virginia 22554.

12. On October 3, 2023, your Affiant received information from UPS Store #7586 that Kimberly Garcia was a regular customer of the UPS Store and that on August 30, 2023, Kimberly Garcia of 4509 Pepperwood Avenue, Long Beach, California 90808 sent a parcel weighing 21 pounds to 900 Providence Street, Stafford, Virginia 22554.

13. Your Affiant is familiar with 900 Providence Street, Stafford Virginia from previous homicide and narcotics investigations. Your Affiant knows that William Dion McQueen, Jr. aka "Draco" / "Duke" uses the address of 900 Providence Street, Stafford, Virginia 22554, which is where his grandmother and brother live. McQueen's current Virginia Department of Motor Vehicle driver's license lists his current address as 900 Providence Street, Stafford, Virginia 22554.

14. On September 7, 2022, William Dion McQueen Jr. was arrested following a homicide investigation. An individual was shot and killed by McQueen in front of McQueen's former residence. McQueen claimed the shooting was in self-defense. However, McQueen was a convicted felon and prohibited from possessing a firearm. During a search of McQueen's former residence pursuant to a search warrant authorizing the search and seizure of evidence related to the homicide, several ounces of marijuana, psilocybin, ammunition, and more than \$40,000 in cash were seized. The \$40,000 was located in a safe, in which your Affiant also found packaging that was consistent with packaging used to ship or mail illicit drugs. The packaging consisted of numerous empty packages that were oblong shaped and consisted of brown packaging tape over numerous layers of plastic wrap with a layer of liquid masking agent in between the layers of plastic wrap. Based on my training and experience, these open empty packages are indicative of illicit drugs being shipped through the mail or common courier for the purpose of redistribution.

15. Further investigation of the caller who checked on Package 1 resulted in a search warrant on October 17, 2023, at 510 Tolbert Loop Stafford, Virginia 22554. During the search of the residence, your Affiant recovered approximately 20,000 "M30" fake oxycodone pills that contained fentanyl, one pound of marijuana, two ounces of cocaine, more than \$46,000 in U.S. Currency and a pistol. The pills were still in the shipping packaging and a resident of the home, Dwaine Jones, had the tracking information for the package in his cell phone. Jones was arrested for possession with intent to distribute fentanyl. Through further investigation, your Affiant determined that the package containing the 20,000 "M30" pills seized from Jones's residence had been sent on October 9, 2023, from Nicole Ramirez of Long Beach, California from UPS Store No. 6490 and was addressed to William Brandon at 16089 Deer Park Drive, Dumfries, Virginia 23025. The package was delivered on October 13, 2023.

16. On December 12, 2023, your Affiant intercepted a parcel being sent to 105 Fiddlers Court in Stafford, Virginia 22554. A search warrant was executed on that package, which was later determined to contain 1000 grams of cocaine.

17. Based on your Affiant's investigation, over the last year your Affiant has located more than a dozen parcels being shipped from the Long Beach, California area from Kimberly Garcia, Nicole Ramirez and Jocelyn Lopez to various addresses in Stafford County, Prince William County and Spotsylvania County, Virginia, all associated with the Dwaine Jones Jr. drug trafficking organization, including the package sent to the SUBJECT RESIDENCE. Based on a review of Jones's telephone records and information provided by Jones at the time of his arrest, your affiant and other agents identified individuals who are facilitating the shipment of fentanyl pills from California to the Eastern District of Virginia. A review of McQueen's telephone toll records shows that McQueen has had regular contact with the same individuals, including one of the main facilitators ("Facilitator"). McQueen's telephone toll records show 20

contacts between McQueen and Facilitator between December 12, 2023, and January 12, 2024. Further investigation revealed that Facilitator has utilized multiple telephone numbers. Your affiant believes that Facilitator has likely changed his phone number again, and your affiant has not yet identified Facilitator's new telephone number. Additionally, following McQueen's arrest on March 19, 2024 (see below), McQueen dropped the phone he was using to communicate with facilitator. Your affiant and other agents are currently trying to identify McQueen's new telephone number. Your Affiant and other agents investigated the names and numbers supplied for Kimberly Garcia, Nicole Ramirez and Jocelyn Lopez, and determined that they are all likely fictitious and used in an effort to thwart identification by law enforcement.

18. On March 16, 2024, your Affiant learned through a police database that William Dion McQueen, Jr. was issued a traffic summons in Miami, Florida. During this incident your Affiant noticed that William Dion McQueen, Jr. was driving a 2021 Rolls Royce Cullinan which returned to Motorcars Leasing out of Miami, Florida. Your Affiant contacted Motorcars Leasing LLC, and based on information provided your Affiant spoke with the current owner of the Rolls Royce, Alexandra Arbelaez. Arbelaez stated that her friend "Mario" is the person who rents out the vehicle for her. Mario stated that he had rented the Rolls Royce to a William Dion McQueen Jr. for 3 days and McQueen had paid around \$1200 per day. Mario said that McQueen had two other individuals with him, for whom McQueen had rented two Lamborghini Uris. Mario said that each of those vehicles also cost \$1200 per day and were also rented for 3 days. Mario said he was not the owner of the two Lamborghinis and he did not have any identification for the other two individuals with McQueen. According to Mario, McQueen paid cash for the 3 vehicles for the 3 days, which would have been \$10,800.

19. On March 20, 2024, your Affiant was contacted by Fairfax County Narcotics Officer D. Horton, who stated that on March 19, 2024, Fairfax County police officers had

arrested William Dion McQueen, Jr. in Fairfax County, Virginia, while driving a stolen motor vehicle. This stolen vehicle was a rental vehicle rented by William Dion McQueen, Jr., that McQueen failed to return. During the course of the arrest, officers observed marijuana residue throughout the passenger compartment of the car and observed a shopping bag on the front passenger floorboard that contained a large quantity of U.S. Currency. An inventory search determined that the bag contained more than \$89,000.00 in cash. When officers asked William Dion McQueen, Jr. about the cash he made no effort to claim it. McQueen was subsequently released on a personal recognizance bond.

20. On March 20, 2024, your Affiant spoke with a confidential source ("CS-1") known to your Affiant, who has provided reliable information to your Affiant in the past. CS-1 stated that William Dion McQueen, Jr. aka "Draco" aka "Duke," has a safe with a large amount of cash, which are profits from drug sales at his grandmother and brother's home, which is located at 900 Providence Street, Stafford, Virginia. CS-1 stated that the brother's name is Dequan McQueen.

21. On March 26, 2024, your Affiant located a receipt from Johnny Dang & Company of Houston, Texas, for William Dion McQueen, Jr.'s purchase of a set of gold and diamond "Grillz." "Grillz" is a term used to describe jewelry that is made to be worn on a person's teeth. This receipt, dated January 10, 2024, shows that William McQueen paid \$19,000.00 for the gold and diamond "Grillz," \$18,500.00 of which was paid in cash and the other \$500.00 was paid with a CashApp account. Attached to the receipt, was a copy of William Dion McQueen, Jr.'s Virginia driver's license. This Virginia driver's license was issued to William Dion McQueen, Jr. on December 17, 2023, and lists his address as 900 Providence Street, Stafford, Virginia 22554. Your affiant obtained a second receipt for the purchase of a white gold necklace "Curly" on January 29, 2024, by William Dion McQueen, Jr. for \$5,000,

which was paid in three installments with CashApp. A subsequent review of McQueen's girlfriend's social media posts revealed a post by McQueen's girlfriend with a picture of a gold necklace in the shape of the word "Curly" on or about February 14, 2024. Subsequent photographs on her social media page include a picture of her wearing the "Curly" necklace and McQueen wearing the "Grillz." Notably, McQueen is wearing a gold necklace that says "Duke," which is one of his nicknames.

22. Your Affiant checked with the Virginia Department of Motor Vehicles (VA DMV) and confirmed that William Dion McQueen, Jr.'s current driver's license has a listed address of 900 Providence Street, Stafford, Virginia 22554.

23. According to the management for Arbor Grove Townhomes, where 900 Providence Street, Stafford, Virginia 22554 is located, the current renters of 900 Providence Street are Robin Griffin, Latoya Griffin, and Dequan McQueen.

24. Your Affiant knows from cellular phone number provided by William Dion McQueen Jr, as his number when he rented the Rolls Royce in March of 2024 and also when he purchased the 'Grillz' in January of 2024 was 571-342-0684. Your Affiant knows from cellular phone toll records for 571-342-0684 that this phone number had been in contact with Robin Griffin, Latoya Griffin and Dequan McQueen as recent as March of 2024. However, following his arrest on March 19, 2024, William Dion McQueen, Jr. dropped this number.

25. I know based on my training and experience that persons who are involved in illicit drug trafficking often carry large amounts of cash. Your Affiant knows that persons who receive shipments of illegal substances across the United States often deposit or ship large amounts of U.S. Currency back to their sources of supply, often using the U.S. Mail or common couriers. It is common for subjects involved in large-scale drug trafficking to launder cash proceeds.

26. Your Affiant knows that individuals involved in large-scale drug trafficking are known to keep records, such as dates and times of shipments, amounts of money owed, fictitious names of senders and receivers, addresses and tracking numbers.

USE OF RESIDENCES BY DRUG TRAFFICKERS

27. Based on my training, experience, and participation in narcotics and drug-related investigations, and my knowledge of this case, I know that:

a. Individuals involved in narcotics trafficking often maintain the following items in their residences: controlled substances and paraphernalia for packaging, weighing, cutting, testing, distributing and manufacturing controlled substances. They will commonly have this contraband on hand, secreted at their premises, on their person, in order to maintain the confidence of their customers as well as to satisfy their own habits. The selling of such contraband is an ongoing type of business, because it takes time to develop clientele, the nature of drug abuse requires a steady supply, and the business tends to be too lucrative to abandon. They also have “fruits” of their illegal sales on hand, including large amounts of United States currency and other valuables.

b. Individuals involved in narcotics trafficking often maintain records of their narcotics transactions and other records of evidentiary value for months or years at a time. It is common, for example, for narcotics traffickers to keep pay/owe sheets or other papers of narcotics sold and monies owed. Such pay/owe sheets or papers are used as a basis for accounting and for settling existing debts. Such records are often maintained for a substantial period of time even after the debts are collected. I have found in my training and experience that such records are invaluable to narcotics traffickers and that such records are rarely discarded. Finally, it has also been my experience that such records and

pay/owe sheets also frequently include the names, identities and telephone numbers of suppliers, customers and coconspirators.

c. Individuals involved in narcotics trafficking must often rely on others to obtain their drugs and to help them market the narcotics. Frequently, traffickers maintain evidence of the identities of these co-conspirators at their residence and their vehicles.

d. Individuals involved in narcotics trafficking often utilize stash houses to store illegal narcotics; weigh, cut and package the illegal narcotics; store narcotics proceeds, and/or store information relating to their drug trafficking business.

e. Individuals involved in narcotics trafficking commonly earn income in the form of cash and try to legitimize these profits. In order to do this, traffickers frequently attempt to secrete, transfer and conceal the money by means, including, but not limited to: placing assets in names other than their own to avoid detection while maintaining control; laundering the money through what appears to be legitimate business or businesses; hiding money in their homes, safes and safety deposit boxes; or using the money to buy assets which are difficult to trace. Records of these and other types of transactions are often found at the residences of individuals involved in narcotics trafficking.

f. Individuals involved in narcotics trafficking often keep and maintain large amounts of United States currency at their residences and in their vehicles. Such funds are often used for every-day expenditures and to maintain and finance their ongoing narcotics business.

g. Additionally, individuals involved in narcotics trafficking often amass and maintain assets at their residence which were generated by their trafficking activities or purchased with the cash earned from such trafficking.

h. Individuals involved in narcotics trafficking often maintain weapons, firearms, and ammunition on their person or in their residence and/or vehicles. Such weapons and firearms are used, and can be used, as an instrumentality of the crime of possession and distribution of drugs and firearms. Furthermore, I am aware of instances in which traffickers have maintained such items in their residences and vehicles in order to protect themselves and guard their drugs, firearms and profits, as well as for enforcement purposes during their narcotics dealings.

i. Residences and premises used by individuals involved in narcotics trafficking usually contain articles of personal property evidencing the identity of person(s) occupying, possessing, residing in, owning, frequenting or controlling the residence and premises.

j. Individuals involved in narcotics trafficking frequently communicate with co-conspirators by means of cellular telephones and electronic devices, such as computers, and usually maintain these items on their person and/or in their residences and vehicles.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

28. As described above and in Attachment B, incorporated by reference herein, this application seeks permission to search for records and items that might be found at the property described in Attachment A, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, including a cellular phone. Thus, the warrant would authorize the seizure and search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

29. *Probable cause.* I submit that if a computer or storage medium, including a cellular telephone, is found at the property described in Attachment A, there is probable cause to believe that it will include evidence, contraband, fruits, and/or instrumentalities of criminal activities for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files or remnants of deleted files may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate and search not only computer files that might serve as direct evidence of the crimes described on the warrant, but also seeks permission to locate and search forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the property described in Attachment A because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer

or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a

computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter- forensic programs or antivirus programs (and associated data) may be relevant to establishing the user's intent.

31. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often

requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data at the property described in Attachment A. Taking the storage media off-site and reviewing it in a controlled environment; however, will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I am applying would permit seizing, imaging, or otherwise copying storage media that reasonably appears to contain some or all the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection to determine whether it is evidence described by the warrant.

33. Because it is possible that more than one person shares the SUBJECT RESIDENCE as a residence, it is possible that the SUBJECT RESIDENCE will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents nonetheless determine that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

34. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID or Face ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours and the passcode or password has not been entered in the last 156 hours. Biometric features from other brands

carry similar restrictions. With Apple devices, a passcode will be required if the phone has five failed attempts to unlock via Face ID. This is often reached by simply handling the phone during arrest or evidence inventory. In addition to device restart as mentioned above, the passcode will also be required after remote activation lock, or when the side or power buttons are pressed for longer than two seconds placing the phone in Emergency SOS mode. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

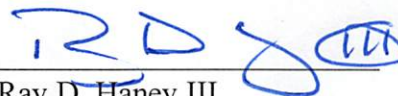
35. Due to the foregoing, if law enforcement personnel encounter any device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant seeks authorization to allow law enforcement personnel to obtain from the aforementioned person the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the finger printscanner of the device(s) found at the SUBJECT RESIDENCE belonging to, or on the person of William Dion McQueen, Jr.; (2) hold the device(s) found at the SUBJECT RESIDENCE and belonging to, or on the person of William Dion McQueen, Jr., in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the device(s) found at the SUBJECT RESIDENCE belonging to or on the person of William Dion McQueen, Jr., in front of the face of the William Dion McQueen, Jr. to activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant. The proposed warrant sought would neither authorize nor prohibit agents requesting that William Dion McQueen, Jr. state or otherwise provide the password or any other means

that may be used to unlock or access the device(s). Moreover, the proposed warrant would neither authorize nor prohibit agents asking William Dion McQueen, Jr. to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the device(s). That is, if agents in executing the warrant ask William Dion McQueen, Jr., for the password to any device(s), or to identify which biometric characteristic unlocks any device(s), the agents will not state or otherwise imply that the warrant requires McQueen to provide such information; that is, the agents will make clear that any such request is strictly voluntary/the person is free to refuse the request.

CONCLUSION

36. Based on the information provided in this affidavit, your Affiant submits that probable cause exists to believe that evidence of conspiracy to commit narcotics trafficking in violation of 21 U.S.C. §§ 841(a)(1) and 846, specifically those items set forth in Attachments B, incorporated by reference herein are contained within the SUBJECT RESIDENCE, as further described in Attachment A, incorporated by reference herein.

Respectfully submitted,



Ray D. Haney III
Task Force Officer
Drug Enforcement Administration

Sworn to before me this 18th day of April, 2024, in Richmond, Virginia.

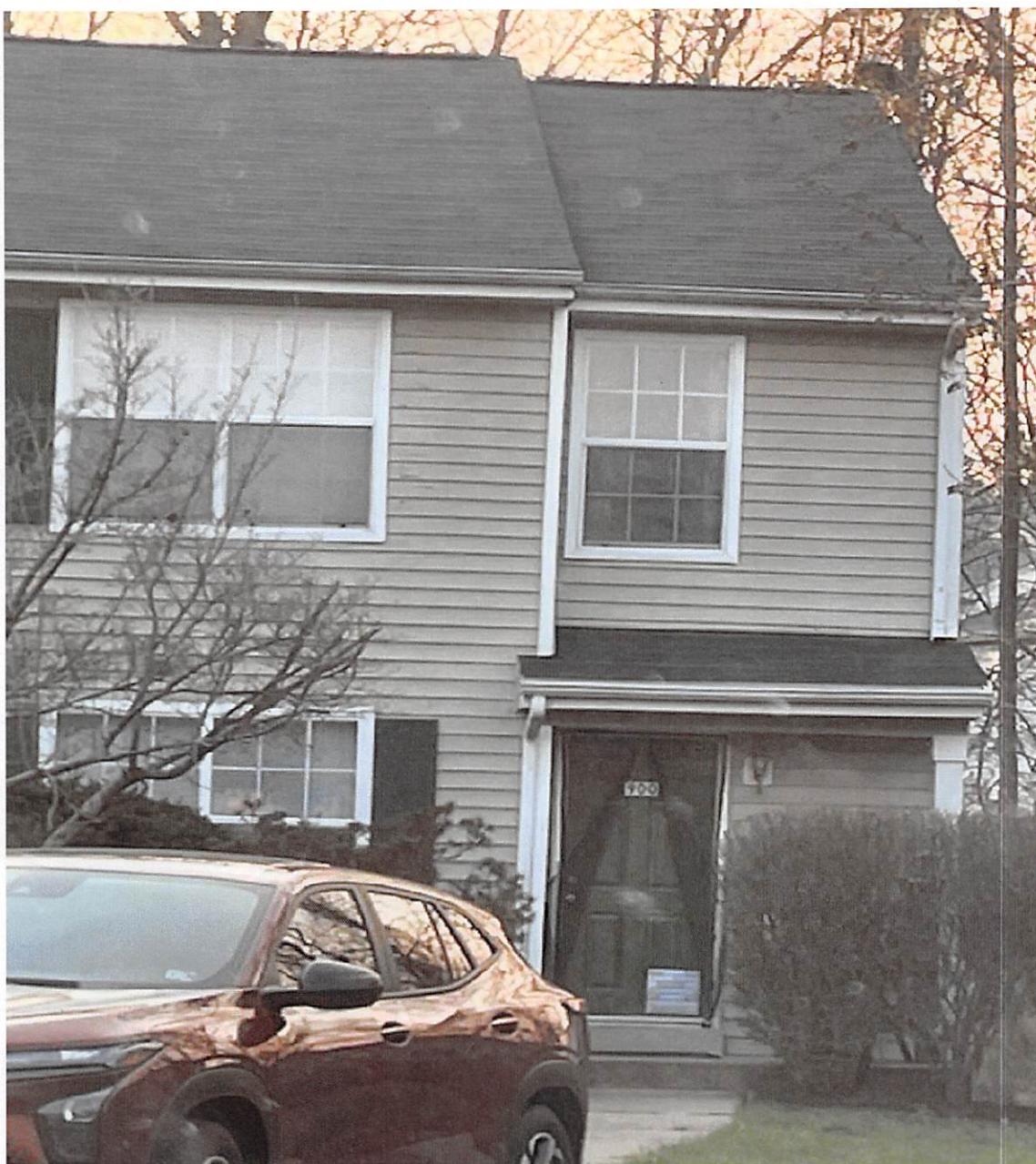


Hon. Summer L. Speight
United States Magistrate Judge

ATTACHMENT A

Place to be searched

The address known as 900 Providence Street, Stafford, Virginia 22554 (“SUBJECT RESIDENCE”) is a two-story single-family townhome located in the Arbor Grove Townhome Complex, that has green colored exterior with white trim. The numbers “900” are black in color mounted on top of a white colored placard on the middle of the door at the main front entrance to the residence. A photograph of the front door exterior of the townhome is below.



ATTACHMENT B

Items to be seized

All items constituting evidence, fruits and/or instrumentalities of illegal drug trafficking in violation of 21 U.S.C. §§ 841(a)(1) and 846, by William Dion McQUEEN, Jr. and others known and unknown including, but not limited to, the following:

- a. Controlled substances, packaging materials, indicia of distribution, records and documents, receipts, notes, ledgers, and other papers including any computerized or electronic records including cellular telephones, relating to the order, shipment, receipt, tracking, purchase, distribution or possession of controlled substances;
- b. Any and all records and information pertaining to the illegal possession or distribution of controlled substances;
- c. U.S. currency and other illicit gains from the distribution of controlled substances, including precious metals, jewelry, and financial instruments;
- d. Books, records, receipts, notes, ledgers, and other papers including any computerized or electronic records including cellular telephones, relating to the order, shipment, receipt, tracking, purchase, distribution or possession of controlled substances and proceeds;
- e. Address and/or telephone books and papers, including computerized or electronic addresses and/or telephone records reflecting names, addresses and/or telephone numbers;
- f. Any and all financial records to include, but not limited to, bank records, checks, credit card bills, account information, and records documenting the receipt and disposition of U.S. currency, or other forms of currency or items of value, related to the order, shipment, receipt, tracking, purchase, distribution or possession of controlled substances.
- g. Books, records, receipts, bank statements, and records, money drafts, letters of credit, money order and cashier's checks, receipts, pass books, bank checks, safety deposit box keys and any other items evidencing the obtaining, secreting, transfer, concealment, storage and/or expenditure of money or other assets including, but not limited to, controlled substances;
- h. Cellular telephones, personal data accessories, computer flash cards, video tapes, compact disks, digital video disks, and other devices and/or electronic media;

- i. Images in all forms, to include video and photographs, and all platforms, including applications, that reference or include the order, shipment, receipt, tracking, purchase, distribution or possession of controlled substances;
- j. Images in all forms to include video and photographs, in particular images showing the association of co-conspirators, of assets, firearms, and of controlled substances;
- k. Any physical or digital record, including but not limited to application and document data, that includes information pertaining to location information or location data;
- l. All notes, application data, or other digital files, to include financial transfers and payments related to the order, shipment, receipt, tracking, purchase, distribution or possession of controlled substances;
- m. Indicia of occupancy, residence, and/or ownership of the subject residence or subject vehicle, including but not limited to, mail, keys, checkbooks, notes, other correspondence, utility bills, rent receipts, payment receipts, bank and other financial statements and records, canceled checks, leases or rental agreements deposit receipts, passports, driver's licenses, social security cards, automobile titles, other identification documents, documents containing personally identifiable information, land and lease titles, escrow papers, photographs, and video and audio records;
- n. Tickets, notes, receipts, and other items relating to domestic and international travel, including but not limited to, airline tickets, boarding passes, airline receipts, car rental agreements, commercial bus tickets, passports, visas and receipts documenting domestic and/or foreign travel;
- o. Cryptocurrency seed phrases, cryptocurrency storage media (i.e., cryptocurrency hardware wallets), and cryptocurrency software wallets;
- p. Records and receipts reflecting the ownership and use of cellular telephones, computers, tablets, pagers, global positioning systems, and cameras;
- q. Safes, both combination and key type, and their contents.

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant ("COMPUTER"):

- a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry

entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. Evidence of the lack of such malicious software;
- d. Evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. Evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;
- f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. Evidence of the times the COMPUTER was used;
- i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. Records of or information about Internet Protocol addresses used by the COMPUTER;
- l. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the SUBJECT RESIDENCE described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of William Dion McQueen, Jr., who is found at the subject residence and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that an occupant state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel an occupant to state or otherwise provide that information. However, the voluntary disclosure of such information by an occupant is permitted. To avoid confusion on that point, if agents in executing

the warrant ask an occupant for the password to any device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the Drug Enforcement Administration (DEA) may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized materials, that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Prosecution Team consists of the agents, taskforce officers, investigators, analysts, attorneys for the government, and personnel designated by an attorney for the government, who are involved in the investigation and prosecution of any cases relating to the instant search warrant.

The Filter Team will have no future involvement in the investigation of this matter, and the Filter Team's work must be overseen and supervised by Assistant United States Attorneys for the Eastern District of Virginia, assigned to the Richmond Division. The Filter Team will review seized communications and segregate potentially protected materials, i.e., communications that are to/from an attorney, or that otherwise reference or reflect attorney

advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team will seek further guidance from the Magistrate Judge issuing the warrant with respect to obtaining a Court Order or other authorization before providing any potentially protected materials to the Prosecution Team. After review and subject to the direction of supervising Attorneys, the Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team. The investigative team may continue to review any information not segregated as potentially privileged.